UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/733,073	12/10/2003	Hugh S. Njemanze	25137-11332	8491

758 7590 04/17/2008

FENWICK & WEST LLP
SILICON VALLEY CENTER
801 CALIFORNIA STREET
MOUNTAIN VIEW, CA 94041

EXAMINER	
DEBNATH, SUMAN	
ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
04/17/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/733,073	NJEMANZE, HUGH S.	
	Examiner	Art Unit	
	SUMAN DEBNATH	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 January 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-5,7-13,15-20 and 22-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5, 7-13, 15-20 and 22-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *08/22/2006 & 01/09/2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-5, 7-13, 15-20 and 22-26 are pending in this application.

2. Claims 1, 9, 16 and 23 are presently amended.

3. Claim 25 has been newly presented in the amendment filed 09 January 2008.

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office Action.

Continued Examination Under 37 CFR 1.114

5. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 09 January 2008 has been entered.

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

7. Claims 1-5, 7-8, 16-20 and 22-24 are rejected under 35 U.S.C. 101 because claimed invention is directed to non-statutory subject matter.

Independent claims 1 and 23 fails to place the invention squarely within one statutory category class of invention. On page 15, paragraph 0037 of the instant specification, the Applicant has provided evidence that the Applicant intends "the software agent" and "manger module" to be software programs which can

be interpreted as software per se. The language of the claim in light of the specification does not meet the definition of the functional descriptive material.

Claims 4-5, 7-8 and 24 are rejected as dependent upon rejected independent claims 1 and 23.

Claims 16-20 and 22, recites different modules of a network system, however these modules can be interpreted as programs per se, thus making the claims recite non-statutory subject matter.

Appropriate correction and/or clarification is required.

Claim Rejections - 35 USC § 103

8. Claims 1-3, 5, 7-11, 13, 15-18, 20 and 22-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Porras et al. (Patent No.: US 6,704,874 B1) and further in view of Pifer et al. (Patent No.: US 4,914,444) (hereinafter "Pifer") and Halstead, Jr. et al. (Patent No.: 5,896,524) (hereinafter "Halstead").

9. As to claim 1, Porras discloses a network security system (abstract) comprising: a first distributed software agent to collect a first stream of alerts from a first network security device having a first clock (FIG. 1, column 3, lines 30-65; column 4, lines 10-22 and column 6, lines 13-17), each alert in the first stream representing an event detected by the first network security device and including a time of detection by the first network security device according to the first clock (column 6, lines 13-17); a second distributed software agent to collect a second stream of alerts from a second network security device having a second clock (FIG. 1, items 12-16 referred to different networks, column 3, lines 30-65; column 4, lines 10-22 and column 6, lines 13-17), each alert in the second stream representing an event detected by the second network security device and including a time of detection by the second network security device according

to the second clock (column 6, lines 13-17); and a manager module in communication with the distributed software agents to receive the first and second stream of alerts (FIG. 1, column 3, lines 62-67 and column 4, lines 10-26), identify a first alert in the first stream and a second alert in the second stream, wherein the first alert includes an Internet Protocol (IP) address, and wherein the second alert includes the IP address (column 6, lines 19-27 and column 8, lines 37-47);

Porras doesn't explicitly disclose to determine, based on the first alert and the second alert, whether the first clock and the second clock are synchronized; and if the first clock and the second clock are not synchronized, synchronize the first clock and the second clock; modifying a least of a timestamp within the first alert and a timestamp within the second alert; and correlate the first alert and the second alert according to a rule. However, Pifer discloses to determine, based on the first alert and the second alert, whether the first clock and the second clock are synchronized; and if the first clock and the second clock are not synchronized, synchronize the first clock and the second clock and correlate the first alert and the second alert according to a rule. (abstract, lines 25-26; col. 2, lines 1-16 and lines 25-30; col. 5, lines 49-52).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Porras as taught by Pifer in order to correlate alerts with sufficient accuracy based on time of occurrence which would help identifying accurate threat level in a given system.

Although Pifer may discloses modifying a least of a timestamp within the first alert and a timestamp within the second alert; and correlate the first alert and the second alert according to a rule (col. 2, lines 34-41 and col. 4, lines 35-40, "event is calculated and used to correct the time of occurrence data for each"), neither Porras nor Pifer explicitly disclose modifying the timestamps within the alerts. However, Halstead discloses modifying the timestamps within the alerts (col. 3, lines 33-37).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Porras and Pifer as taught by Halstead in order to reduce amount of processor instructions since if the current timestamp of an alert and/or event falls into the allowable range no further work would be needed to identify the event.

10. As to claims 9, 16 and 23, these are rejected using the same rationale as for the rejection of claim 1.

11. As to claims 2, 10, 17 and 24, Porras discloses the network security system wherein the manager module determines a synchronization error using the time of detection including the first alert and the time of detection included in the second alert (column 6, lines 18-27 and column 8, lines 37-51). Porras doesn't explicitly disclose synchronizing the first clock and the second clock and correcting the synchronization error. However, Pifer discloses synchronizing the first clock and the second clock and correcting the synchronization error (abstract, lines 25-26; col. 2, lines 1-16 and lines 25-30; col. 5, lines 49-52). Furthermore, Pifer discloses determines a synchronization error using the time of detection including the first alert and the time of detection included in the second alert (abstract). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Porras as taught by Pifer in order to correlate alerts with sufficient accuracy based on time of occurrence which would help identifying accurate threat level in a given system.

12. As to claims 3, 11 and 18, Porras doesn't explicitly disclose synchronizing the first clock and the second clock by selecting one of the first and second clocks as a reference clock, and adjusting the other clock to the reference clock. However, Pifer discloses synchronizing the first clock and the second clock by

selecting one of the first and second clocks as a reference clock, and adjusting the other clock to the reference clock (col. 2, lines 1-16 and lines 25-30; col. 5, lines 49-52). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Porras as taught by Pifer in order to correlate alerts with sufficient accuracy based on time of occurrence which would help identifying accurate threat level in a given system.

13. As to claims 5, 13 and 20, Porras doesn't explicitly disclose synchronizing the first clock and the second clock by adjusting a time offset associated with the first clock. However, Pifer discloses synchronizing the first clock and the second clock by adjusting a time offset associated with the first clock (col. 2, lines 1-16 and lines 25-30; col. 5, lines 49-52). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Porras as taught by Pifer in order to correlate alerts with sufficient accuracy based on time of occurrence which would help identifying accurate threat level in a given system.

14. As to claims 7, 15 and 22, Porras discloses the network security system wherein the second alert is corroborative of the first alert (column 6, lines 13-27 and column 8, lines 37-51).

15. As to claim 8, Porras discloses the network security system wherein the first network security device comprises an Intrusion Detection System (IDS) (column 2, lines 18-38).

16. As to claim 25, Porras discloses further comprising causing the event represented by the first alert to occur (column 2, lines 18-38).

17. As to claim 26, Porras discloses further comprising causing the event represented by the second alert to occur (column 2, lines 18-38).

18. Claims 4, 12 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Porras in view of Pifer, Halstead and Apel et al. (Patent No.: US 6,760,687 B2), hereinafter Apel.

19. As to claims 4, 12 and 19, neither Porras and Pifer nor Halstead explicitly discloses wherein selecting one of the first and second clocks comprises determining a relationship of the first and second clocks to a system-wide reference clock. However, Apel disclose wherein selecting one of the first and second clocks comprises determining a relationship of the first and second clocks to a system-wide reference clock (column 9, lines 8-15 and lines 60-65). Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Porras, Pifer and Halstead by selecting one of the first and second clocks comprises determining a relationship of the first and second clocks to a system-wide reference clock as taught by Apel in order to provide a highly accurate and flexible system.

20. Examiner's note: Examiner has cited particular columns and line numbers in the references as applied to the claims above for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may be applied as well. It is respectfully requested from the applicant, in preparing the responses, to fully consider the references in entirety as potentially teaching all or part of the claimed invention as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Response to Amendment

21. Applicant has amended claims 1, 9, 16 and 23, which necessitated new ground of rejections. See rejection above.

Conclusion

22. Any inquiry concerning this communication or earlier communications from the examiner should be directed to SUMAN DEBNATH whose telephone number is (571)270-1256. The examiner can normally be reached on 8 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/S. D./
Examiner, Art Unit 2135
/KIMYEN VU/
Supervisory Patent Examiner, Art Unit 2135